BNA

Privacy and Security Law Report®

Privacy and Data Protection in Turkey: (Inching) Towards a European Framework

BY OMER TENE AND YUCEL SAYGIN

Introduction

With a population of 73 million, second only to Germany when compared to the 27 European Union Member States, and a gross domestic product growth rate of 8 percent, Turkey is a force to be reckoned with on the outskirts of Europe. Turkey harbors the largest city in Europe (Istanbul, with an estimated population of 15 million); has 63 million mobile telephone subscribers; and is the fifth largest country in the world in terms of the number of Facebook users (after the United States, Indonesia, India, and the United Kingdom) with 30 million.

Yet despite many years of political and public debate, Turkey remains without a comprehensive legal framework for privacy and data protection. Besides constituting an obstacle in Turkey's quest to become a member of the European Union, the lack of a modern data protection law limits business opportunities and potential collaboration between Turkish and foreign businesses and law enforcement entities and compromises the fundamental rights of Turkish individuals.

Omer Tene is managing director, Tene & Associates, and Associate Professor, Israeli College of Management School of Law. Yucel Saygin is a professor of engineering and natural sciences at Sabanci University, Istanbul. Both are participants in MODAP (Mobility, Data Mining, and Privacy), a Coordination Action project funded by the EU FET OPEN.

Constitutional Amendments

In March 2010, the Turkish government submitted to Parliament a package of constitutional amendments, including an amendment to the privacy protection provision, Article 20, adding a section on data protection.[1] The constitutional amendments were authorized by the unicameral Turkish Grand National Assembly in May 2010, yet failed to garner the support of a two-thirds majority required to pass directly, gaining 336 of the 500 members of Parliament, short of the 367 threshold. They were therefore submitted to a nationwide referendum in September 2010, after withstanding constitutional challenge in the Turkish Constitutional Court, where they passed with sweeping support of 58 percent of the vote.

Pursuant to the constitutional amendment, Article 20 now states that ''everyone shall have the right to the protection of their personal data.''[2] It provides that personal data may only be collected, stored, and used pursuant to a legal obligation or with the data subject's consent. It grants individuals the right to be informed about any processing of their personal data, as well as the right to access, rectify or delete their personal data. It calls for legislation setting forth the principles and procedures to implement the constitutional mandate. Yet even before such legislation is put in place, Turkish individuals benefit from constitutional protection *vis-à-vis* action by public sector bodies. Indeed, in its latest progress report, the European Commission states that

[1] The text added to Article 20 of the Turkish Constitution provides: ''Everyone has the right to demand the protection of his personal data. This right comprises the right to be informed about the personal data concerning himself, access to such data, right to request correction or deletion of them as well as the right to be informed if such data is [sic] used in accordance with the purposes for which it was collected. Personal data can be processed only in cases regulated in a law and upon express consent of the subject individual. Principles and procedures regarding the protection of personal data shall be regulated by a law.''

[2] Communications secrecy continues to be protected by Article 22 of the Constitution.

 ISSN 1538-3423

''with regard to fundamental rights, progress has been made. Constitutional amendments bring important changes in the area of data protection (. . .).''[3]

Finally, Turkey is currently in the process of introducing a new Constitution to replace the existing document, which dates from 1982, a relic of the 1980 *coup d'état*.[4] Given that privacy and data protection are not politically controversial, we hope that the new Constitution will echo the provisions of the recently amended Article 20.

Omnibus Legislation

Omnibus data protection legislation has been contemplated in Turkey for almost a decade, but has been slow in coming. Turkey is a signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (''Convention 108''), yet has not ratified the Convention. It is has also been a member of the Organization for Economic Co-operation and Development (OECD) since 1961. As part of Turkey's 2005 Accession Partnership with the European Union, Turkey was required to ''adopt a law on protection of personal data'' and ''establish an independent supervisory authority.''[5]

According to the European Commission's 2009 progress report, Turkey is yet to take the required measures to implement this data protection agenda. The Commission stated: ''With regard to respect for private and family life and, in particular, the right to protection of personal data, Turkey needs to align its legislation with the data protection *acquis*, in particular Directive 95/46/EC, and, in that context, to set up a fully independent data protection supervisory authority. Turkey also needs to ratify both [Convention 108] and the additional protocol to it on supervisory authorities and transborder data flow (CETS No 181). Wiretapping has reportedly been used extensively and records of it published in the press.''[6] In its 2010 progress report, the Commission emphasized that an ''effective personal data protection regime is crucial for efficient international judicial cooperation.''

In 2003, the Turkish Ministry of Justice tabled a Draft Law on the Protection of Personal Data (the ''Draft Law''); yet the Draft Law has since been lost in parliamentary committee hearings, while Turkey remains without proper legislation. The Draft Law is predicated on the European Data Protection Directive (95/46/EC). It applies ''to natural and legal persons whose personal data are processed'' and defines personal data as ''any information relating to an identified or identifiable natural or legal person.'' Hence, unlike most European data protection laws, the Draft Law would protect both individuals and legal entities. Similar to European data protection legislation, it applies to both automated and manual data processing. The Draft Law sets forth principles for the processing of personal data, including purpose specification, proportionality, accuracy, and retention limitation. It lists legitimate bases for processing personal data, including consent and compliance with a legal obligation.

Article 7 of the Draft Law, which applies to sensitive data, permits processing ''[i]f the personal data are required to be processed for purposes of preventive medicine, medical diagnosis, medical treatment, health care or execution of health services by: (1) Health facilities, (2) Insurance companies, (3) Social security institutions, (4) Employers with the liability of establishing [a] health unit at the work place, (5) Schools and universities; in accordance with the relevant laws, under the supervision of health care personnel (. . .).'' We believe that this provision, which is based on Article 8(3) of the European Data Protection Directive, is overly broad. It exposes highly sensitive data not only to health care providers but also to insurance companies, social security institutions, employers and schools; indeed, it is difficult to foresee *any* use of medical data that is not authorized by Article 7. As such, it lacks adequate safeguards to protect the privacy of patients and their families. Hence, even if it is pushed through the legislative process, the Draft Law remains deficient.

Other provisions in the Draft Law appear internally inconsistent. For example, under Article 5(2) of the Draft Law, ''[p]ersonal data can be re-processed for scientific or statistical purposes or for a longer duration than stated (. . .), provided that there [are] adequate safeguards in the relevant legislation regarding the purpose of re-processing (. . .).'' Thus, this provision allows processing of data for secondary purposes, including scientific or statistical purposes, without expressly requiring that such data be anonymized. At the same time, Article 10 of the Draft Law provides that ''[f]or research, planning and statistical reasons which aim at public benefit, the personal data can be processed provided that they are made anonymous.''

Additional provisions of the Draft Law provide individuals with rights of transparency, access and rectification (Articles 11–13) and impose data security obligations (Article 15), as well as restrictions on cross-border data transfers based on the principle of adequacy (Article 14). Certain provisions of the Draft Law already appear outdated, such as those setting up a registry of databases (Articles 16–19). Even in Europe, the bedrock of the database registration (notification) regime, regulators have come to accept that in a globalized economy with ubiquitous data flows, such bureaucratic exercises yield few tangible benefits. The Draft Law further sets up a data protection authority as well as an independent data protection board (Articles 26–33), although the relation between the two is not entirely clarified by the legislative text. Finally, the Draft Law sets forth penal, administrative and civil causes of action for willful or negligent unlawful processing of data.

---

[3] Commission Staff Working Document, Turkey 2010 Progress Report, accompanying the Communication from the Commission to the European Parliament and the Council, Enlargement Strategy and Main Challenges 2010-2011, 9 November 2010, http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/tr_rapport_2010_en.pdf.

[4] Ece Toksabay, the Turkish prime minister, wants new Constitution by the first half of 2012, Al Arabiya News, Sept. 29, 2011, available at: http://www.alarabiya.net/articles/2011/09/29/169270.html.

[5] Council Decision 2008/157/EC of 18 February 2008 on the principles, priorities and conditions contained in the Accession Partnership with the Republic of Turkey and repealing Decision 2006/35/EC, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:051:0004:01:EN:HTML.

[6] Commission Staff Working Document, Turkey 2009 Progress Report, accompanying the Communication from the Commission to the European Parliament and the Council, Enlargement Strategy and Main Challenges 2009-2010, 14 October 2009, http://ec.europa.eu/enlargement/pdf/key_documents/2009/tr_rapport_2009_en.pdf.

  PVLR ISSN 1538-3423

Almost a decade has passed since the introduction of the Draft Law—a very long time in terms of technological progress and business development. Innovations and breakthroughs, particularly in information and communications technologies, have created new business models and tools affecting individuals' lives and impacting the functioning of virtually every business process and government activity. This means that the Draft Law is in danger of becoming obsolete even before its enactment. Indeed, the EU Data Protection Directive, which serves as its main model, is subject to comprehensive review by the European Commission this year. In devising its data protection legislative strategy, Turkey should take account of these transformations to avoid adopting an outdated scheme.

Sector-Specific Regulation

With omnibus data protection legislation stalled and the establishment of a data protection authority delayed, Turkey has begun developing sector-specific regulatory schemes. First and foremost is the framework for the protection of privacy and personal data in electronic communications. In 2000, Turkey established the Telecommunications Council as the institution responsible for data protection in the telecom sector. The Council was responsible for the enactment in 2004 of the By-Law on Personal Data Processing and Protection of Privacy in the Telecommunications Sector (the ''Regulation'') as well as the 2008 By-Law on Security of Electronic Communications. The Regulation is based on the principles of the European e-Privacy Directive (2002/58/EC), such as communication confidentiality and security, the handling of traffic and location data, call number identification, public subscriber directories, and the prevention of spam.

In the past few years, the Council, now named the Information and Communications Technology Authority (''ICTA''), has enforced the Regulation forcefully, imposing steep penalties and making its presence felt in the telecom sector. In one case, *Taraf*, a Turkish newspaper, disclosed that personal data of subscribers of a telecom operator could be accessed by third parties. After a thorough investigation, ICTA issued the operator a fine in an amount of TL 1.25 million ($800,000). Another case involved illicit access by a former Turkish soccer star, Ridvan Dilmen, to call traffic records of his ex-girlfriend. An investigation launched by the ICTA and carried out by the police ultimately led to the imposition of a fine in an amount of TL 13 million ($9 million) against Turkcell, which has the largest number of users of any mobile provider in Turkey.

Additional sector specific legislation applies in the financial sector, under the Banking Law of 2005, which imposes a strict duty of confidentiality subject to criminal and civil sanctions, and the Bank Cards and Credit Cards Law of 2006, which restricts retention or re-use by retailers of customer information as a result of credit transactions.

Alas, at the same time, many sectors of the Turkish economy remain largely unregulated, including important government projects such as electronic health records, which contain highly sensitive information about patients' prescription histories and lack adequate measures of privacy and data protection. For example, the Turkish Ministry of Health established a comprehensive Medication Tracking System (''MTS'') for purposes such as ensuring drug safety, accounting for use of medications and engaging in pharmacovigilance. The MTS is based on a Ministry of Health regulation titled ''Medicine Tracking and Evaluation.'' Under this scheme, massive amounts of personal data, including name, age, diagnoses, hospital visited, medicines purchased, and adverse effects, are collected and stored in a centralized database. Not only health care practitioners but also pharmacists are able to query the database about a patient's prescription history, as well as additional information, such as address and social security payments. Even more sensitive health data are collected and stored by Turkey's Social Security Administration.

The Medicine Tracking and Evaluation regulation fails to clearly articulate: the purposes for collection of patients' data, roles and responsibilities of various actors involved, procedures for reporting adverse medicine effects to third parties, and scope of access authorizations. Moreover, the MTS appears to violate data protection principles such as proportionality and data minimization, collecting large amounts of personal data and making them available to numerous parties without apparent necessity. It is evident that only comprehensive data protection legislation can quench the thirst of public sector entities for additional data and subject such entities to requirements of data minimization, security, and retention limitation.

Moving Ahead

In order to give substance to the latest constitutional amendments and progress toward harmonization and partnership with the European Union, Turkey should adopt data protection legislation based on the fair information principles (''FIPs'') set forth in the 1980 OECD Privacy Guidelines. In addition, Turkey should establish a privacy and data protection authority charged with enforcing data protection legislation against both the private and public sector, in a manner commensurate with the structure of Turkey's constitutional and administrative law.

While procedures for implementation and enforcement diverge, there is broad global consensus concerning the substantive data protection principles, such as purpose limitation, proportionality, transparency, and security. Indeed, even the United States, which does not yet have across the board data protection legislation, has recently endorsed regulation based on the FIPs. In its Report on ''Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,'' the U.S. Department of Commerce states: ''To provide consistent, comprehensible data privacy protection in new and established commercial contexts, we recommend that the United States Government recognize a full set of Fair Information Practice Principles as a foundation for commercial data privacy.'' Turkey, which has already recognized the importance of protecting the right to privacy and individuals' data in its constitutional amendment and acceded to Convention 108, should likewise adopt legislation setting forth the FIPs as statutory requirements. The FIPs should apply to both private and public sector entities and be enforced by a dedicated data protection authority.

Turkey's data protection authority should be established in a manner commensurate with its constitutional and administrative law. Under a recent decree, Turkey subjected all independent regulatory bodies to

the supervision of government ministries.[7] While the EU Data Protection Directive mandates a supervisory authority acting ''with complete independence,'' independence should be balanced against enforcement powers and accountability. Turkey's legal system favors strong enforcement agencies exercising broad powers and that are accountable to the judiciary branch over weak independent authorities effectively acting as ombudsmen. The European Commission approved the ''adequacy'' of data protection frameworks in Argentina and Israel, despite these countries' data protection authorities being integrated into the executive branch.[8] A similar structure, where the data protection authority is subject to strictly financial and administrative oversight of the Ministry of Justice, should be considered in Turkey.

Conclusion

Despite constitutional amendments and the establishment of a strong regulator in the field of telecom privacy, Turkey continues to lack a comprehensive data protection framework in the mold of EU Member States. This imbalance, subjecting a specific sector of the economy to what has sometimes been considered heavy-handed regulation, while leaving other sectors without regulatory guidance or oversight, should be corrected. A data protection authority, established in the spirit of European regulatory agencies and empowered to enforce the law in all sectors of the economy as well as against the state, would correct this imbalance and propel the Turkish economy towards European standards.

---

[7] Independent bodies in Turkey attached to ministries after new decree law, Hürriyet Daily News, Aug. 22, 2011, http://www.hurriyetdailynews.com/n.php?n=independent-bodies-in-turkey-attached-to-ministries-after-new-decree-law-2011-08-22.

[8] *See, e.g.*, Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, OJ L 27/39, 1 Feb. 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF.

  PVLR ISSN 1538-3423